

Abstract of the Disclosure

A smart card is ideally suited for applications such as
5 retail loyalty, cash replacement, membership, physical access,
network/information security, healthcare, vending,
transportation, and couponing. In fact, a single card can manage
and deliver multiple applications. It is this powerful concept
which will shape the eventual success and wide spread acceptance
10 of smart cards. This "sharing" of a card, however, presents
numerous challenges for keeping the application data separate and
retaining ownership. This invention describes a method for the
secure allocation and control of card resources. Specifically,
the application providers can be given control over their own
15 specific application domain while the card issuer still retains
ultimate ownership control of the card and therefore can dictate
what applications can be loaded. Although there exists some
techniques for managing applications on a virtual machine smart
card using advanced cryptography, this invention discloses an
20 approach that will work on conventional file system smart cards.

Each application will have its own space on the card
firewalled from the others. Further, these applications can be
securely added or removed dynamically even after the file system
card is in circulation. In particular, a method is disclosed for
25 organizing the structure of the card so that different
applications are secure and separate. As well, the permission to
create and load these applications can be granted exclusively by
the card issuer. This is accomplished through a series of one
time only keys which can be selectively disclosed to application
30 providers. By presenting the keys in the prescribed manner the
application provider will be able to unlock the card for the
purposes of loading new application files. After each load the
key is rotated to a new value that is randomly generated. This

serves to relock the card and prevent unlicensed groups from piggybacking applications onto the card.

Application providers such as banks, health insurers, retailers, local transit authority can now be confident that
5 their application is secure from unauthorized use.

This method opens up an entirely new business model for conventional, non-cryptographic low cost smart cards. A State can issue an ID card and then authorize selected agencies to load applications, a shopping mall can offer a card onto which mail
10 retailers can load their own unique loyalty programs, and banks that issue credit/debit cards can now license out space to partner organizations.